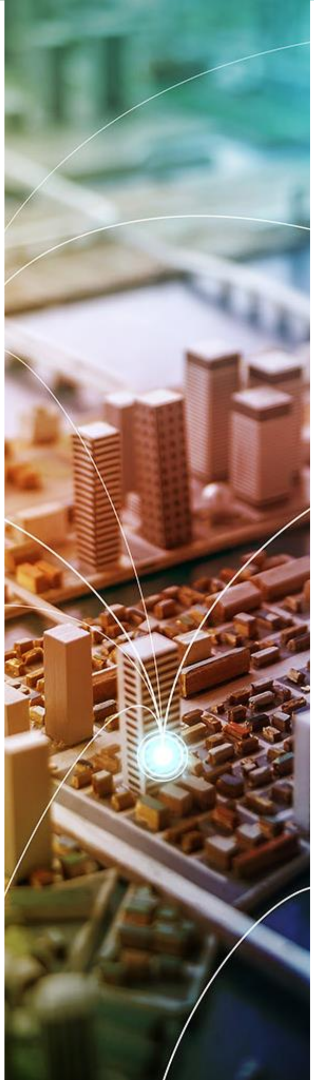
Rambus

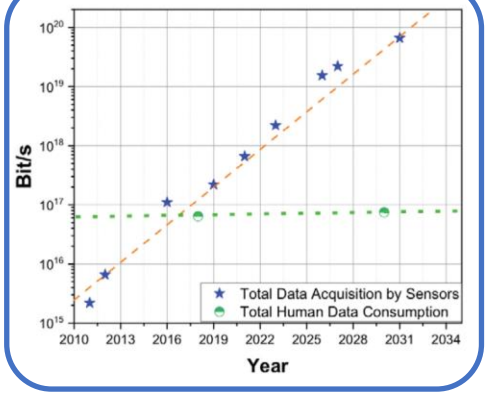
Emerging Security Challenges in Highly Interconnected Semiconductor Systems

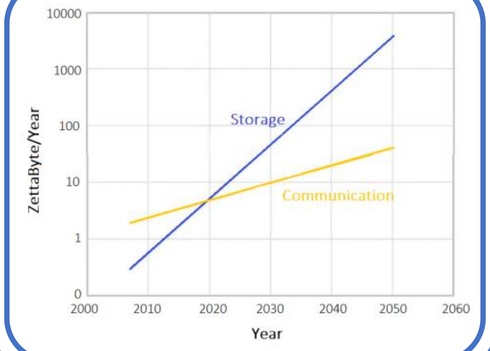
Neeraj Paliwal

April 27, 2023



Why Does Security Matter Even More Today?





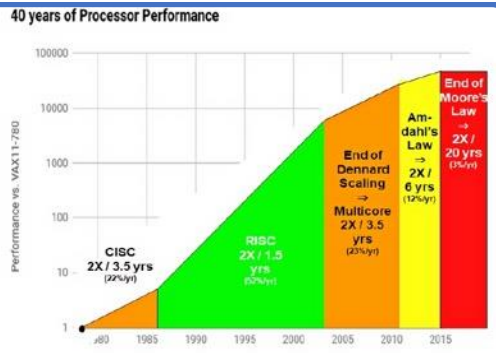
(Source: SRC, Decadal Plan For Semiconductors)

Increased complexity and fragility of the supply chain driven by emerging suppliers and technologies such as 3D chips and systems, (multi-) chiplet integration, stacking etc.,

Exponential increase of data acquisition rate per sensor. Total data acquisition has been estimated to reach 10^{27} bytes-per-year by 2032 (>10^20 bit/s)

Paradigm shift from "move data to compute" to "move compute to data" driven by the alarming growing gap between the world's technological informational storage need and the communication capacity

Why Does Security Matter Even More Today?



Moore's law is slowing

AI demands are growing

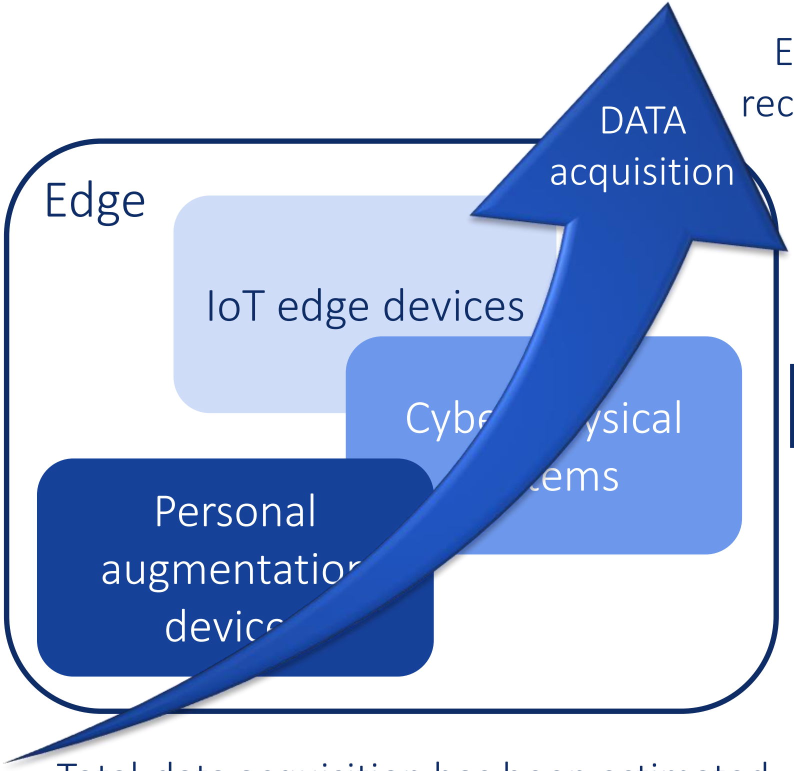
General purpose CPUs and GPUs can't meet the performance demands of today's AI workloads

AI workload optimized "heterogeneous compute" architecture is driving the demand for new chips

These new chips are developed by emerging system design companies instead of the traditional ones

Many designs focus on AI performance and may find their chips vulnerable without a reliable IP supplier

Emerging Trends: From Data Centers to DATA Everywhere



Exponential growth of recorded data at the edge

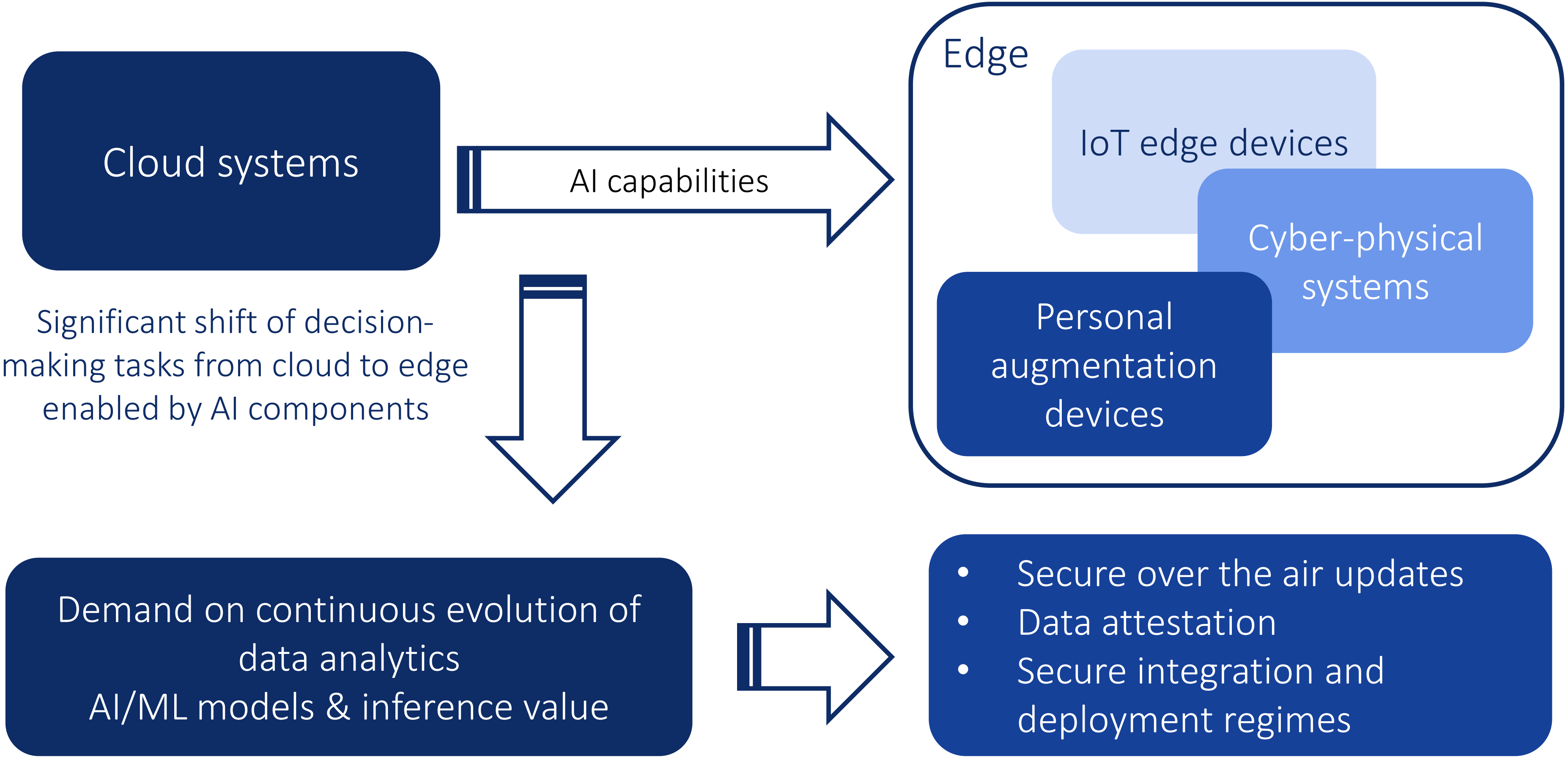
Only 25% of the acquired data will be housed in a data center

Total-data acquisition has been estimated to reach 10^27 bytes-per-year by 2032

A paradigm shift is required to admit data at the edge into economic activity:

- Move the compute to the data
- Security in the broadest sense:
  Protection, Trust and Control

AI Capabilities: From Cloud to Edge



Security at the Edge: Challenges

- Edge devices are in the field
  - Easier to access for adversaries
  - Non-expert users
    - Devices are supposed to help / entertain, not create work
  - Wide-ranging environment interactions
    - Example: Troop locations revealed by fitness trackers
- Governments have taken notice: Regulation
  - Privacy (e.g., GDPR)
  - Health (e.g., HIPAA Security Rule)
  - Automotive Cyber Security (e.g., UNR 155 & 156)
  - US National Cyber Security Strategy
  - EU Cyber Security Act & EU Cyber Resilience Act
  - Government purchasing requirements (e.g., FISMA, EO14028)

HEALTHCARE & PHARMA MARCH 22, 2019 / 1:10 AM / UPDATED 4 YEARS AGO

FDA says cybersecurity vulnerabilities found in some [redacted] devices

By Reuters Staff 1 MIN READ

Car thieves are hacking key fobs to quickly and quietly steal vehicles

by Bettie Cross | Thu, May 12th 2022, 11:49 PM GMT+2

This picture is from a keyless car theft in England. One crook goes to the front door where a lot of people store their key fobs. The signal from the key fob is amplified and relayed to a second device that's being held close to the car door. The car is tricked into thinking the key fob is next to the door. That allows the car to be opened, started and driven away. (Photo: West Midlands Police)

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BABY YOU CAN DRIVE MY CAR —

Gone in 130 seconds: New [redacted] hack gives thieves their own personal key

You may want to think twice before giving the parking attendant you[redacted]issued NFC card.

DAN GOODIN - 6/8/2022, 10:21 PM

Back in 2015, [redacted] said the intrusion involved malicious software installed on cash registers at some of its resort restaurants, gift shops and other payment systems that *were not* part of the its guest reservations or membership systems.

'Satori' IoT Botnet Operator Pleads Guilty

September 4, 2019 51 Comments

A 21-year-old man from Van operating the "**Satori**" botnet was built to conduct massiv platforms and Web hosting

SOCIETY | GERMANY

[redacted] says sabotage behind massive train disruption

10/08/2022

Th[redacted] blamed cable sabotage for a major train disruption and said security authorities had taken over the investigation. It had earlier reported that the "technical fault" had been repaired.

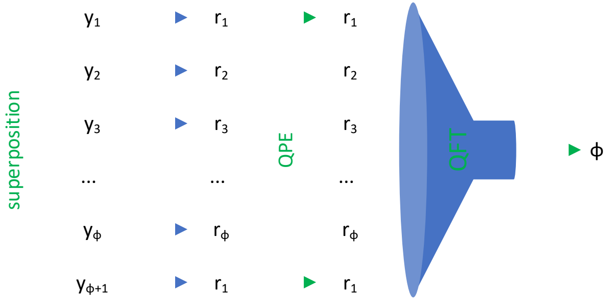
Traditional Security is the Basic Layer at the Edge

- Securing cryptographic keys
  - ✓ Root of Trust
  - ✓ Secure Element
- Securing firmware and over the air updates
  - ✓ Secure boot
  - ✓ Package / update managers, signed updates
- Securing IDs
  - ✓ Biometrics
  - ✓ Password managers
- Secure development processes
  - ✓ Limit attack surface by fighting feature creep
  - ✓ Vulnerability scanners and vulnerability disclosure routines
  - ✓ Established, high quality code base (libraries)

We know how to do this!
“Just” need to deploy it.

A Very High-Level View of Shor's Quantum Algorithm

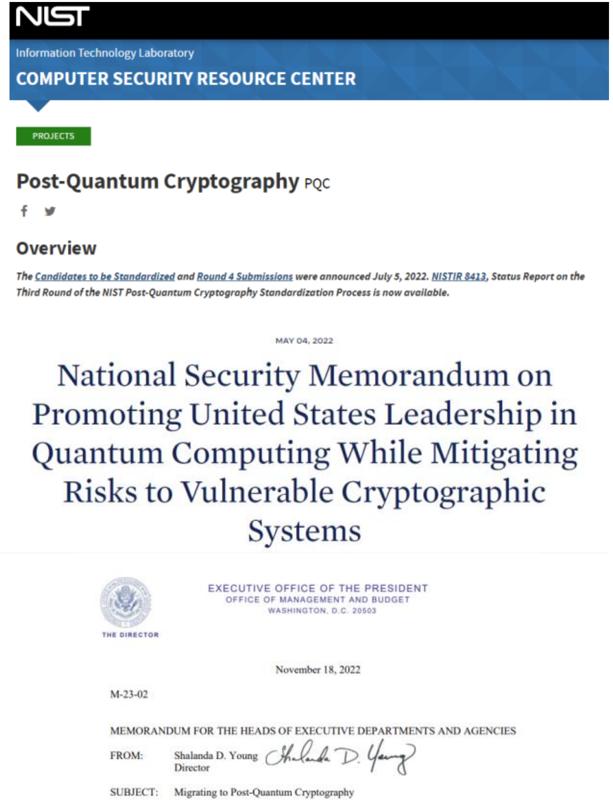
- To break RSA, we need to learn secret primes p, q from public N (we know $N = pq$)
- From number theory, we know that for suitable x, $r \equiv x^y \bmod N$ is periodic
  - i.e., $r \equiv x^y \bmod N \equiv x^{y+\phi} \bmod N \equiv x^{y+2\phi} \bmod N \equiv \cdots$
- From number theory, we further know that $\phi \in \{1, p-1, q-1, (p-1)(q-1)\}$
- Quantum superposition enables (relatively) efficient Quantum Phase Estimation (QPE)
- Quantum Fourier Transform (QFT) allows extracting binary integer ϕ from QPE results



- Small number of repetitions needed until suitable x found

Updating the Traditional Security: Quantum-Secure Crypto

- Quantum Computers threaten RSA, ECC
  - Digital signature algorithms must change
  - Session key establishment algorithms must change
- Use cases determine when the change must happen
  - Mosca's Theorem: Everything is good as long as $t_u + t_s < t_q$
    - t_u: Time to update devices, networks and applications
    - t_s: Time that data needs to be secure
    - t_q: Time until quantum computers large enough
- Transition to Quantum Secure Crypto is a massive effort
  - All IoT devices / services will be affected
- Governments around the world push to hasten transition
- Standardization in progress but no standards yet
  - Except for secure boot (LMS, XMSS)


NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography PQC

Overview

The Candidates to be Standardized and Round 4 Submissions were announced July 5, 2022. NISTIR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process is now available.

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

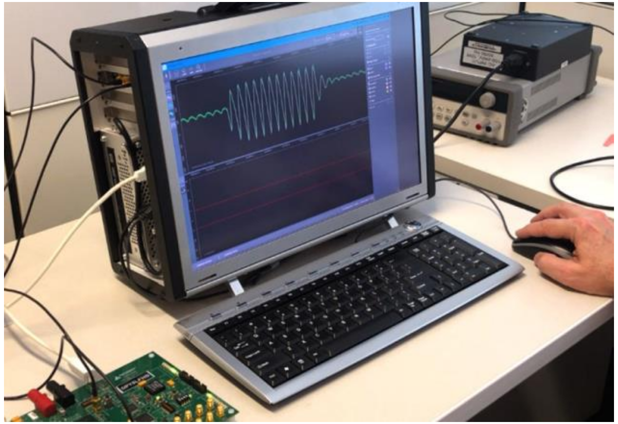
FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

Rapidly evolving situation – challenging everyone for the next 15 years

Physical Attacks at the Edge

- Service interruption
  - Disrupting cables, wireless is cheap
  - Need to plan infrastructure with human adversaries in mind
- Side-channel attacks
  - Measure power / EM / time / … of computation
  - "Look inside" operations, exploit sensitive intermediates
  - More powerful than normal adversaries
- Targeted fault-injection attacks
  - Authentication bypass (e.g., ID and firmware checks)
  - Key extraction (e.g., faulted cryptographic operations)
  - Data dumps (e.g., pointer manipulation)
  - Can even abuse device features like power scaling



Glitch it if you can: parameter search strategies for successful fault injection

Rafael Boix Carpi[1], Stjepan Picek[2,3], Lejla Batina[2], Federico Menarini[1], Domagoj Jakobovic[3] and Marin Golub[3]

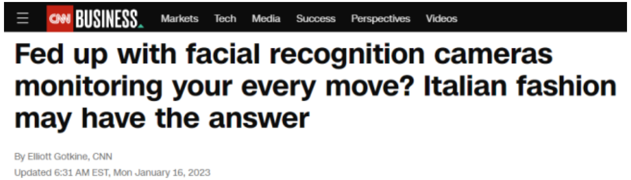
[1] Riscure BV, The Netherlands, {BoixCarpi, Menarini}@riscure.com
[2] Radboud University Nijmegen, The Netherlands {s.picek, lejla}@cs.ru.nl
[3] Faculty of Electrical Engineering and Computing, Zagreb, Croatia {domagoj.jakobovic, marin.golub}@fer.hr

Abstract. Fault analysis poses a serious threat to embedded security devices, especially smart cards. In particular, modeling faults and finding effective practical approaches that are also generic is considered to be of interest for smart card industry. In this work we propose a novel

Robust knowledge foundations but most markets only catching up.

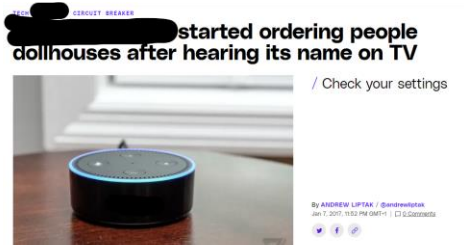
Security at the Edge: Attacking AI

- Artificial Intelligence derived from biological models
  - Natural intelligences can be tricked – used for education, psychological healing, marketing, abuse
  - No inherent countermeasures against malicious inputs in AI either


CNN BUSINESS Markets Tech Media Success Perspectives Videos

Fed up with facial recognition cameras monitoring your every move? Italian fashion may have the answer

By Elliott Gotkine, CNN
Updated 6:31 AM EST, Mon January 16, 2023


TECH [redacted] CIRCUIT BREAKER

[redacted] started ordering people dollhouses after hearing its name on TV

/ Check your settings

By ANDREW LIPTAK / @andrewliptak


BBC Sign in Home News Sport Reel Worklife

NEWS

Home | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science | Stories

Tech

[redacted] chatbot is taught to swear on Twitter


TECH

'They're All So Dirty and Smelly:' Study Unlocks [redacted] Inner Racist

Researchers found racist beliefs are baked into [redacted] and the chatbot will tell you all about it with a few simple tweaks.

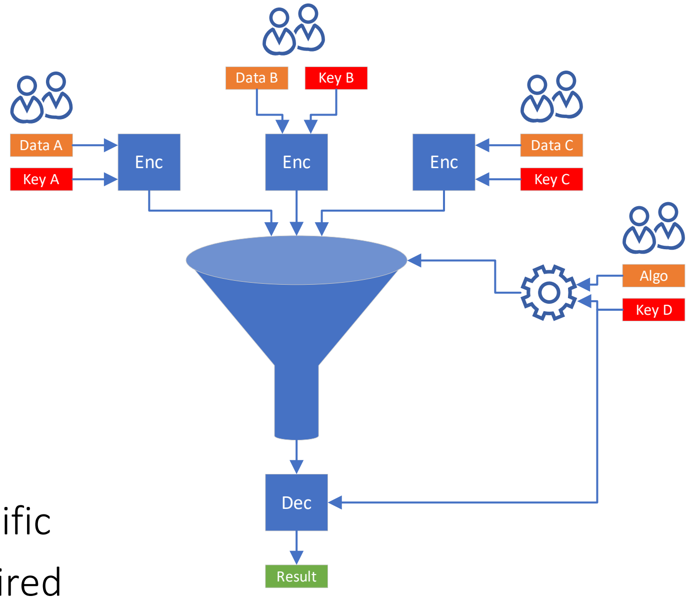
By Thomas Germain Published April 13, 2023 | Comments (28) | Alerts

- At edge, additional attacks are possible
  - Proprietary AI models are a form of content that requires protection against pirates
  - Content pirates know how to use side-channel attacks
  - Content pirates know how to use fault-injection attacks
  - AI models increasingly mission critical – denial of service particularly easy at edge

Ongoing research topic

Security at the Edge: Securing Computations

- At the edge, you find:
  - Proprietary data from multiple sources
  - Proprietary analysis algorithms processing data
  - Vulnerable devices
- Advanced cryptography provides solution:
  - Fully-Homomorphic Encryption (FHE)
  - Multi-Party Computation (MPC)
  - Basic idea: Compute only on encrypted data
  - Basic idea: Use cryptographic means to scramble algorithms
  - Current situation: Practicality of schemes very use-case specific
  - Current situation: Limited useability, expert knowledge required
  - Current situation: First deployments in networking, ad auctions, genome research



Emerging technology, not ready for general purpose deployments yet.

Security at the Edge: Securing Sensors

- For car keys: long history of distance bounding solutions and attacks
  - Relay attacks allow adversaries to unlock cars even if key is far away
  - Distance bounding tries to ensure that key is near car
  - Basic idea: derive distance measurement from response times
  - Current situation: Cat-and-mouse between defenders and adversaries
- Fundamental problem:
  - Cryptography is mathematical, measurements are physical
  - Cryptography derives its strength from reductions to mathematically “hard” problems
  - Measurements for IoT can not be reduced to physical equivalent of “hard” problem
  - Any IoT sensor will can be fooled by sufficiently motivated engineer
  - Faulty sensor inputs will always be a problem for AI in IoT

Major challenge

Summary

- Compute and data are moving into highly interconnected edge devices

$ Edge devices are increasingly driving business critical applications

✓ We can deploy solid basic security for edge devices

! But risks are larger due to edge exposure and basic security is not enough
  - Many challenges are work in progress
  - AI at the edge adds its own challenges
  - Advanced cryptography is providing new opportunities
  - Need to account for risks that cryptography can not solve

Thank you

Rambus
Data · Faster · Safer